electronics

MDPI

Article

Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks

Ruben Fratty, Yuval Saar, Rajnish Kumar * and Shlomi Arnon

Department of Electrical and Computer Engineering, Faculty of Engineering Sciences, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel
* Correspondence: rajnish@post.bgu.ac.il

Abstract: The recent expansion of networks of low-earth orbit (LEO) satellites such as Starlink, OneWeb, and Telesat and the evolution of communication systems toward B5G and 6G with densely interconnected devices could generate opportunities for various cyber attacks. As the satellite network offers many crucial services to the public and governmental organizations, cyberattacks pose severe risks to the communication infrastructure. In this study, we propose a random routing algorithm to prevent distributed denial-of-service (DDoS) attacks on an LEO satellite constellation network. The routing algorithm utilizes the classical algorithms, i.e., k-DG, k-DS, k-SP, and k-LO, by introducing randomness and selecting one with weighted probability distribution to increase the uncertainty in the algorithm. The study shows that the proposed random routing algorithm improves the average and median cost of the attacker against DDoS attacks while maintaining the functionality of the network. The algorithm is optimized by formulating a Bayesian optimization problem. In addition to providing an additional level of uncertainty in the routing, there is an improvement of 1.71% in the average cost and 2.05% in the median cost in a typical scenario. The algorithm causes the network to be robust to cyber attacks against LEO Satellite Networks (LSNs), however, similar to any other defensive measures, it reduces the network's goodput.

Keywords: cybersecurity; distributed-denial-of-service attacks; LEO satellite network; routing algorithm

Citation: Fratty, R.; Saar, Y.; Kumar, R.; Arnon, S. Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks. *Electronics* **2023**, *12*, 518. https://doi.org/10.3390/electronics12030518

Academic Editor: Cheng-Chi Lee

Received: 7 December 2022
Revised: 13 January 2023
Accepted: 17 January 2023
Published: 19 January 2023

1. Introduction

The interest in LEO satellite networks (LSNs) is increasing with the recent launches from SpaceX, Oneweb, Telesat, and Globastar [1]. The modern LSN consists of hundreds of satellites in orbit, causing it to be a dense network that will provide seamless communication services to public and government agencies. These dense LSNs aim to provide optical fiber-like Internet services with lower latency [2,3]. Satellites provide a myriad of services including communication, broadcasting, GPS and navigation, banking, Internet of Things (IoT), early warning systems, meteorology, remote sensing, and surveillance [4,5]. With the increasing role of LSNs in the communication infrastructure, several security issues have begun to appear at the forefront that have been largely neglected so far [6,7]. One of such issues is the increasing cyberattacks on satellite networks, which will be detrimental to the communication infrastructure and cause a lot of damage to service providers, the end users, and governments.

Distributed Denial of Service (DDoS) attacks, which have been a huge threat to the Internet since its early days, have been used effectively for a while against satellite networks. In [8], the authors show that a DDoS attack is feasible in the LSN and that the traditional mitigation and prevention methods are ineffective because of the special characteristics of these networks. The research on such attacks is an ever-going battlefield between attackers constantly modifying their tools and defenders modifying their approaches to oversee new attacks. In 2015, 20% of businesses with 50 or more employees suffered at

least one DDoS attack and 26% of DDoS attacks led to data loss [9]. Especially in the satellite communication sector, the DDoS attack frequency increased by 255% from the second half of 2018 to first half of 2019 and increased yet again by 295% from the first half of 2019 to its second half [10]. The typical results of such an attack include network infrastructure, service continuity, and business reputation damages. Furthermore, these can have devastating costs, e.g., the average cost of downtime for an enterprise can reach up to USD 2 million [11].

There are three kinds of satellite networks: Geosynchronous equatorial orbit (GEO), Medium earth orbit (MEO), and LEO satellite. The GEO satellites are located at an altitude of 36,000 km from the earth and remain fixed in the sky when observed from the ground. Due to larger distances, they have higher propagation losses and transmission delays besides not able to cover high latitude areas [12]. The non-geostationary satellites have recently gathered more attention due to seamless connectivity, lower propagation delays, lower expense, and broadband communication [13,14]. The NGSO satellites include the MEO at altitudes between 8000 and 20,000 km and LEO between 400 and 2000 km above earth. Recently, several mega-constellations of LEO satellites have been launched by Starlink, Telesat, Globastar, Oneweb, and Iridium that will provide connectivity and broadband communication services [15]. The LSN offers lower transmission delay and propagation losses causing it to be attractive for ultra-reliable low-latency communication. However, there are significant challenges in the routing algorithms of LSNs. The routing in terrestrial networks relies on the routing tables obtained from the network topology that leads to greater network overhead and slow convergence [16]. Besides, the demands of computational power and storage can be met for these routers. However, in the case of LSNs, the network topology is dynamically varying and has limited onboard computation and storage. The high mobility of LEO satellites causes instability in the established paths [17].

In [18], the authors describe how a new architecture called NDN (Named Data Architecture), which is already being considered instead of traditional TCP/IP architecture, may solve that problem of mobility in the inter-satellite links. They also consider how the knowledge of the relative position of each satellite in the grid may be beneficial to forwarding NDN packets. Another challenge is presented in the form of the topology of the network as shown in [19]; the authors show that network topology has a big impact on the type of routing algorithm that should be used, e.g., Delay-Tolerant Network (DTN) or non-Delay-Tolerant Network (non-DTN). The routing strategy in such a dynamic network will depend on the density of the network and the mobility pattern. As the density of nodes increases, the probability of finding the paths increases and hence the Non-Delay-Tolerant Network (Non-DTN) is more suitable for enhancing the performance of routing protocols. The Delay Tolerant Network (DTN) protocols are more favorable in the case of low density and high mobility [19]. In [20], the authors offer a realistic uplink framework designed to imitate real satellite network performance issues such as satellite availability, packet collision, and interference. This implies that those are actual challenges that routing protocols try to mitigate. The capacity of the ground-to-satellite link is another major challenge, being subject to various atmospheric fading mechanisms that cause it to be a bottleneck of the entire network. Some challenges of routing algorithms in LEO satellite networks arise from unbalanced traffic distribution among the nodes of the network, which may lead to surges of activities in some areas. This is studied in [21] using a two-hops state-aware routing strategy based on deep reinforcement learning (DRL-THSA).

The key factors that cause LSNs to be more vulnerable to attacks compared to terrestrial networks include: (a) satellite locations are largely available to the public and are therefore easier for an adversary to specifically target, (b) low latency requirements limit different path options and cause routing to be more predictable, and (c) their reliance on the cyber networks and the Internet for functioning. However, some other factors that work in the favor of LSNs are: (a) the ever-changing nature of inter-satellite networks that cause the attacker a risk of two attacks congesting each other rather than the target inter-satellite link

and (b), as the number of end users connected to the satellite will be much smaller than the Internet, it requires on the part of the adversary a very efficient, careful, and planned use of resources for DDoS attacks.

Broadly, the solution to the cyberattacks can be categorized into two types: (a) Physical layer solution and (b) cryptography-based solutions. The physical layer solution takes advantage of the the physical properties of the channel and wave propagation to secure the network against the eavesdropper while the cryptographic solution utilizes the encryption algorithms.

Some of the works that focus on physical layer solutions are as follows. In [22], the authors have investigated the eavesdropping in Non-Geostationary Orbit (NGSO) communication systems in the physical layer and derived the closed form expression for channel secret capacity and outage probability while considering the effect of rain attenuation. In [23], the authors have investigated the secrecy performance of a land mobile satellite channel with shadowed-Rician fading. An attempt to solve the confidentiality problem in the network coding of multi-beam satellite systems has been studied and, using semi-definite programming, the sum secrecy rate was optimized by designing optimal beamforming [24]. In [25], the authors have minimized the total transmit power of a satellite while satisfying the user's secrecy rate for a scenario in which the legitimate receivers are placed among multiple beams while being surrounded by many passive eavesdroppers. The investigation of the secrecy outage probability of a hybrid satellite–terrestrial relay network (HSTRN) in the presence of multiple eavesdroppers is studied in [26]. In [27], the authors have studied beamforming and artificial noise methods for securing hybrid satellite–terrestrial networks. The investigation of the secrecy performance of a satellite wiretap channel assuming a Shadowed Rician fading is performed in [28]. In [29], the authors have investigated the physical layer security performance of hybrid satellite and a free-space optical (FSO) cooperative system. In [30], the Doppler shift and received power characteristics of an LEO satellite are used to differentiate between the legitimate and illegitimate satellites using support vector machines.

On the other hand, some of the works that focus on cryptography techniques to secure satellite communication systems include: a demonstration scheme for an architecture of a satellite communication using the SAFEcrypto cryptographic solutions [31], utilization of elliptic curve cryptography in the design of a three-factor authentication protocol for satellite communications that is meant to secure the communications against well-known attacks [32], a novel encryption algorithm using XOR operation [33], and a parallel architecture Authenticated Encryption (AE) algorithm for high-data throughput optimized for satellite applications [34].

However, as the communication systems will evolve to the future generation of communication networks, e.g., B5G and 6G, we will need various cross-layer solutions to address the cyberattacks on the densely connected network. More recently, several works began to appear that focus on securing satellite communications in a scenario with respect to DoS/DDoS attacks using the network layer solution. A proof-of-concept was introduced in ICARUS dealing with distributed denial-of-service attacks in the context of LEO satellite networks [8]. In [35], the authors have described mechanisms for supporting Quality-of-Service (QoS) strategies that consider the properties of LEO satellite networks and provide an explanation about several QoS routing strategies as well as their difference from traditional best-effort routing algorithms. In [36], the authors have proposed a strategy named Directed Percolation Routing (DPR) that they used for providing Ultra-Reliable and Low-Latency Communication (URLLC). In [37], a lightweight risk avoidance routing algorithm is proposed to avoid forwarding the user's data in a high-risk area. In [38], the authors have used an active distributed QoS routing strategy with consideration being given to the link duration to find the optimum path.

In this work, we address the DDoS attacks on LSNs based on a network layer solution by proposing a random routing algorithm. The algorithm randomly selects among many algorithms to choose with a weighted probability distribution. This ensures that the cost of

attacks launched from several bots leading to a DDoS attack is increased due to the increased uncertainty in the LSN routing algorithm. The network layer solution proposed in this work will be applicable for the increasing modern dense network of LEO satellites vulnerable to DDoS attacks. In Figure 1, we show the scenario depicting the launch of a DDoS attack from several compromised bots against LEO satellite networks. The contribution of the article can be summarized as follows:

(1) We propose a k-RAND algorithm that selects from one of the four algorithm—k-DG, k-DS, k-SP, and k-LO—to maximize the average cost of the attacks while maintaining the functionality of the LEO satellite communication network.
(2) To optimize the performance of our proposed algorithm, we formulate a Bayesian optimization problem that will maximize the average cost of the routing algorithm for DDoS attacks.
(3) We show that the average cost of the DDoS attacks on the satellite network is enhanced with the optimized k-RAND algorithm.

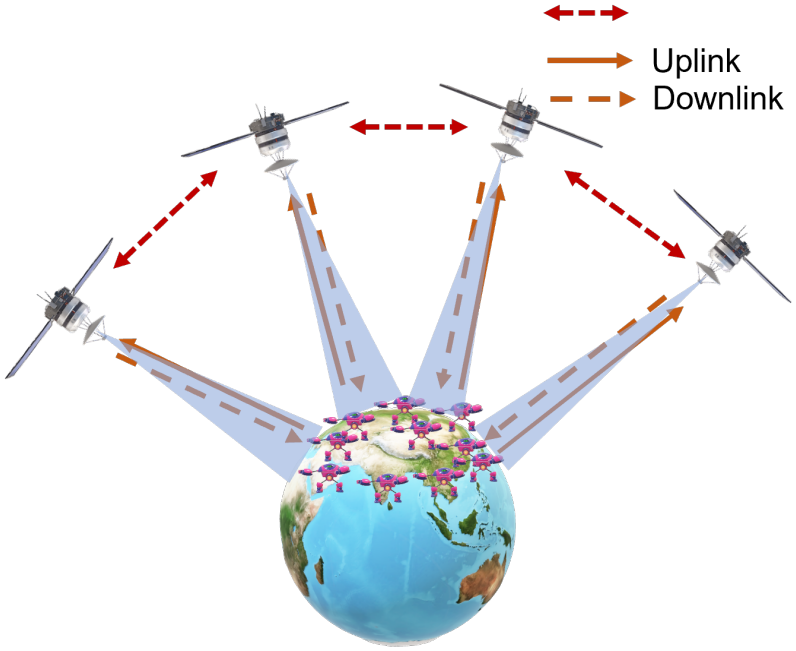

Figure 1. DDoS attacks on LEO satellite network launched from several compromised bots.

The rest of the article is organized as follows: In Section 2, we briefly discuss various kinds of cyberattacks on an information system in the context of satellite communication networks. In Section 3, we discuss the proposed random routing algorithm and the Bayesian optimization problem formulation to optimize the performance. Section 4 presents the numerical simulation and discussion. In Section 5, we conclude the paper.

2. Cyberattacks in Satellite Networks

Broadly, attacks on satellite communication networks can be classified into two types: (a) electronic attacks and (b) cyberattacks [39]. The electronic attacks target the electronic devices through which the system transmits and receives data. Such electronic attacks include jamming and spoofing. On the other hand, cyberattacks target the data directly and the systems using the data. A cyberattack refers to the deliberate and nefarious attempt to breach a information system for malicious purposes [40].

Cyberattacks can be used to take control of information systems and devices, intercept, eavesdrop on, and corrupt data. The antennas on satellite stations and ground stations, as well as the systems connecting ground stations to satellite networks, are all potential entry points for hackers to launch cyberattacks [41]. Attacks that target data interception attempt to store data as it is transmitted through a satellite information system or eavesdrop

the flow of data over the connected network [42]. An attacker will be able to verify the success of their security breach attempt in almost real-time, even if a satellite service provider is unaware of the attack while it is happening or even after it has occurred. During a data corruption attack, malicious software, such as malware, is introduced into the system and the data are altered to purposefully display incorrect information. As hackers may successfully conceal their identities and carry out completely irreversible attacks, these types of crimes are challenging to identify and track.

Cyberattacks can potentially be used to gain access and control of an orbiting satellite system and ultimately be able to execute commands on the satellite communication systems onboard. Such types of attack will be extremely difficult to attribute and the repercussions will be irreversible if the attacker gains complete control of the systems and alters or makes changes in a way that may cause severe unrecoverable damage. The service provider might take notice of the attack but would not be in a position to take any affirmative action as it will be too late to reverse the damage. Such attacks, which include gaining complete control of satellites, can cause severe collateral damage and may lead to the disabling of the target satellite, leaving it to drift in its orbit in uncontrolled fashion or even worse the path can be slightly drifted and cause collisions with other satellites. We now briefly summarize various kinds of cyberattacks.

- Denial-of-service (DoS) and DDoS attacks: The attacker will overwhelm or flood the information system in such a way that leads to a denial of service to the intended legitimate users. The attack is typically carried by a single computer or device. The DDoS attack is a type of DoS attack in which the attacker uses several distributed devices to flood the data traffic. The distributed devices are usually compromised bots [43].
- Man-in-the-middle (MitM) attack: The attacker places itself in the communication link between two parties in order to intercept, eavesdrop, or corrupt the data being exchanged between the involved parties. Such an attack will enable the attacker to steal login passwords and personal information and spy on the victim [44].
- Phishing and spear-phishing attacks: Phishing attacks are based on using social engineering and technical tricks to manipulate the users. The attackers disguise as a trusted party to send emails and messages that will lead to the installation of some malicious software or the revealing of personal and sensitive information. A spear-phishing attack is a targeted attack by gathering some typical information about the target users or organization to increase the probability of success of a phishing attack. As this attack is very specific and targeted, it is difficult to identify and defend against [45].
- Drive-by attack: Such attacks are a common way to install and download malicious software without any explicit permission from the user. This usually happens while visiting a compromised website that will automatically download and install to infect the device, steal information, or corrupt stored data. This is also known as a drive-by download as this does not require any action on the part of victim. A drive-by download attack can take advantage of the security vulnerability of an app, operating system, or web browser [46].
- Password attack: Passwords are required to obtain access to an information system, storage devices, and emails. Password attacks use special techniques and software to guess the passwords of users to gain access to their system. Such access to a user's password can be obtained by smart guessing by combining date of birth, place of birth, pet's name etc., using social engineering and tricks and gaining access to a password database [47].
- SQL injection attack: Structured Query Language (SQL) attacks are mostly common with database-driven websites. The attacker inserts SQL commands that can lead to access, modify, and delete databases or completely shut them down [48].
- Cross-site scripting (XSS) attack: XSS attacks inject malicious code into a trusted website. The users visiting the website will be vulnerable to give away personal information or download software onto their computers [49].

- Eavesdropping attack: Eavesdropping attacks occur by intercepting, modifying, or deleting the data that are being exchanged between two parties. It takes advantage of an unsecured communication network to snoop on the data transfer in transit [50].
- Malware attack : Such attacks uses malicious or unwanted software designed to harm the information system. It can lead to stealing, deleting, or encrypting the data, gaining access and control of the device, locking the device, and injecting some spy software. Some examples include virus, worm, ransomware, trojan horse, bots, spyware, adware, etc. [51].

For launching a DDoS attack on the LEO satellite network, the attacker will use several compromised bots/users located on the ground by combining various kinds of cyberattack techniques to gain access or control of the end users on the ground spread across a vast geographical area. After gaining complete control of these users, it can flood and overwhelm the data traffic of the downlink/uplink or inter-satellite link of the satellite communication link to deny services to the genuine users.

3. Random Routing Algorithm

In the context of densely connected LEO communication networks, an attacker can easily plan a DDoS attack to congest an inter-satellite communication link. This is expected due to the fact that when the routing algorithm is deterministic, and with the assumption that the attacker knows the algorithm as well as the network grid (each satellite's location), it is feasible to predict how the network will route a packet in the inter-satellite communication network. This is also supported by the ICARUS study. One way to address the challenge could be to add randomness in the routing algorithm that will cause it to be more difficult for the attacker to successfully perform a DDoS attack. First, we define the following two terms in the context of attacks: cost and MaxUp.

The cost of an attacker is defined in the following way: how many resources in terms of traffic volume (Gbps) an adversary has to use in order to be successful in achieving the attack's goal. For example, if one bot generates 10 Mbps of traffic volume, then the ISL capacity of 10 Gbps would mean 1000 bots transmitting 10 Mbps each to the ISL network.

Detectability/MaxUp is defined as follows: If the attacker just targets one satellite to launch its attacks then a sudden change in traffic volume to a single node in the network would be easily noticeable. To avoid such detectable situation, attackers distribute their traffic volume over several satellites in the LSN by placing several bots on the ground. Therefore, the detectability/MaxUp is defined as the maximum absolute change in the bandwidth caused by the attacker across the LSN for the up-link transmission.

When the algorithm is less deterministic, this means that the attacker has to send more packets in order to congest the target ISL. This is expected to happen as the attacker has to cover a greater number of cases probabilistically. The transmission of more packets over the network means increasing the cost (sending more packets from multiple ground stations/bots) or the MaxUp (sending more packets from a single ground station). For example, let us assume that the routing algorithm is a BFS (breadth-first search). Given a grid of satellites and a source and destination of ground stations, this algorithm will return a similar path no matter how many times it is being run. For the attacker, that means it knows the exact route of each packet sent, which in turn allows the attacker to only send as many packets as needed to congest a target ISL.

On the other hand, assume the algorithm returns the three shortest paths leading from the source to the destination. Now, the attacker must take into account every possible short path, which may be more than just three. That means the attacker has to send more packets. If the attacker sends more packets from the source station that would increase the MaxUp since more traffic from a single station is easier to recognize. The attacker can alternatively send more packets from multiple other ground stations, but that would increase the cost since the attacker would need to have a larger botnet to have access to more ground stations. In conclusion, sending more packets means increasing the cost (sending more packets from multiple ground stations) or MaxUp (sending more packets from a single ground station).

In order to add randomness to the routing algorithm, we select one of four algorithms to be used with weighted distribution. These four algorithm are chosen from the algorithms evaluated in ICARUS and already implemented in the framework: k-DG, k-DS, k-SP, and k-LO. These algorithms include [8]:

- Shortest paths (k-SP): The k-sp algorithm finds k paths between the source and destination in the network with the minimum length [52]. This algorithm distributes traffic among the k-shortest paths in the satellite communication network [53].
- Ground-to-ground disjoint paths (k-DG): The algorithm considers k-shortest paths with node disjoint paths, i.e., without any shared uplinks, downlinks, or inter-satellite links. The node disjoint paths only share the source and destination points [54].
- Satellite-to-satellite disjoint paths (k-DS): This algorithm finds the k shortest paths with the node disjointness forced only on the inter-satellite links while allowing overlaps in the paths of the uplinks and the downlinks.
- Limited-overlap shortest paths (k-LO): The algorithm finds the k shortest path between the source and destination ensuring that these paths are sufficiently dissimilar to each other. It is an implementation of the ESX algorithm, as shown in [55], in that it finds the k shortest paths with a similarity score of less than 50%.

The proposed random algorithm k-RAND is summarized in Algorithm 1. We generate a random variable A between 0 and 1. For the values of A between 0 and a_1, we select the shortest path (k-SP) routing algorithm; for values between a_1 and a_2, k-DG is selected and so on. The values of a_1, a_2, and a_3 will be determined based on the maximization of the statistics of the cost of attack. There will be a trade-off between these two competing measures (cost and MaxUp) for the DDoS attacks against LSNs.

Algorithm 1 k-RAND algorithm

```
Generate A randomly between [0, 1]
  If 0 ≤ A < a1
    Use shortest paths (k-SP)
  Else If a1 ≤ A < a2
    Use sround-to-ground disjoint paths (k-DG)
  Else If a2 ≤ A < a3
    Use satellite-to-satellite disjoint paths (k-DS)
  Else
    Use limited-overlap shortest paths (k-LO)
```

In order to find the parameters of the proposed k-RAND algorithm, i.e., a_1, a_2, and a_3, we formulate a Bayesian optimization problem. The Bayesian method is a derivative free approach to find the minima of expensive-to-evaluated functions. The cost function of the optimization is the average cost of the DDoS attacks on the LSN. The solution is then obtained using the Bayesian approach [56,57].

$$\min_{a_1,a_2,a_3} \quad C_{avg} \tag{1}$$

where C_{avg} denotes the average cost of attacks.

4. Simulation Results and Discussion

In this section, we show the simulation results and compare the performance of the proposed random routing algorithm with some of the most widely used routing algorithms (k-DG, k-DS, k-LO, and k-SP) as shown in [8]. The study has been performed in the LSN framework of ICARUS [8] that uses a simulation performed on the Starlink constellation consisting of 1584 satellites. The values of a_1, a_2, and a_3 have been obtained after 50 iterations using the Bayesian optimization algorithm and the best values are found to be 0.377, 0.403, and 0.412, respectively. This algorithm is the one that proved to be the most

efficient in increasing the cost while maintaining a good MaxUp. The probability mass functions (PMFs) of the four algorithm are shown in Table 1.

Table 1. PMF of Algorithms.

Algorithm	PMF
k-SP	0.377
k-DG	0.026
k-DS	0.009
k-LO	0.588

In Figure 2, the histogram plot of the attackers' costs for the considered LSNs are shown. The frequency in the plot refers to the bin frequency. The cost is normalized with respect to the one ISL bandwidth that is 20 Gbps. The cost includes the feasibility of the attack on the downlinks and inter-satellite link of the LSN. As for the case of the uplink attacks, the compromised bots have to be in the coverage area of a given satellite and hence the MaxUp is very high, meaning the attacks will be easily detectable. We can observe that the proposed algorithm is able to increase the cost of the attacks so that the attacker has to deploy more scattered compromised bots probabilistically to lead to a successful attack. The average and median of the cost of attack is shown in Table 2. It is to be noted that the k-RAND provides the optimum median and average cost while maintaining a good functionality over the network. Compared to the k-SP, it provides an improvement of 1.71% in the average cost and 2.05% in the median cost. In the case of a dense LEO satellite communication network, such a percentage would matter as the DDoS attacks must be distributed over a larger area to be less detectable. Concentrating the attack in a certain area will be easily detectable as there will be significant traffic increase in that particular area. Probabilistically, the attacker also will have uncertainty in the choice of the particular routing algorithm used and this will, therefore, force them to utilize more network traffic.

Table 2. Cost statistics.

Algorithm	Average	Median
k-SP	0.9107	0.9480
k-DG	0.9088	0.9665
k-DS	0.9168	0.9635
k-LO	0.9264	0.9665
k-RAND	0.9262	0.9675

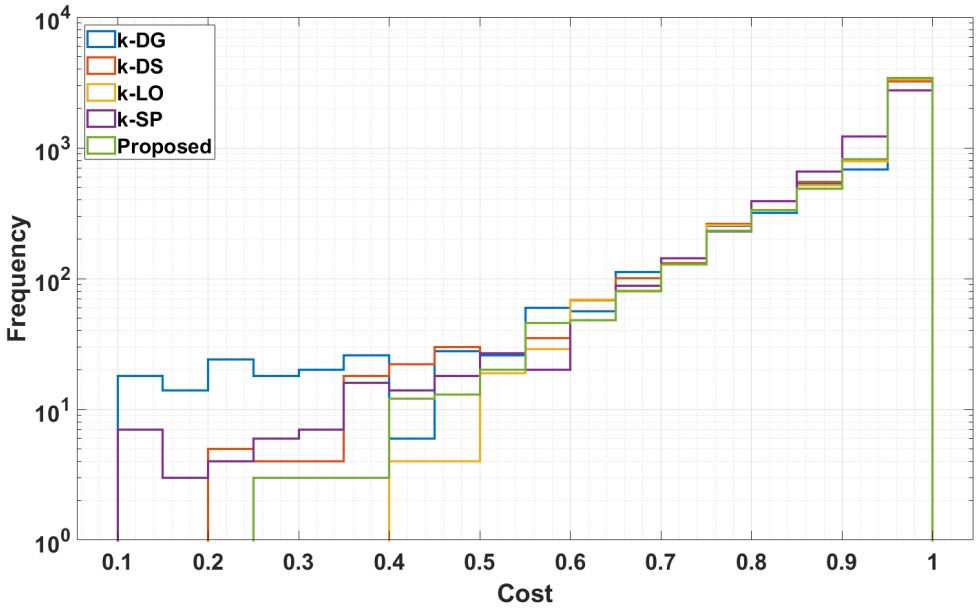

Figure 2. Histogram plot of the attackers' costs of launching DDoS Attack on an LEO satellite network.

Figure 3 shows the cumulative distribution function (CDF) of the cost of the attacks with the considered algorithms. The CDF denotes the empirical distribution function and is defined as:

$$F_n(x) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}_{X_i \leq x} \tag{2}$$

where X_i are the sample observations, n is the number of observations, and $\mathbb{1}$ denotes the indicator function.

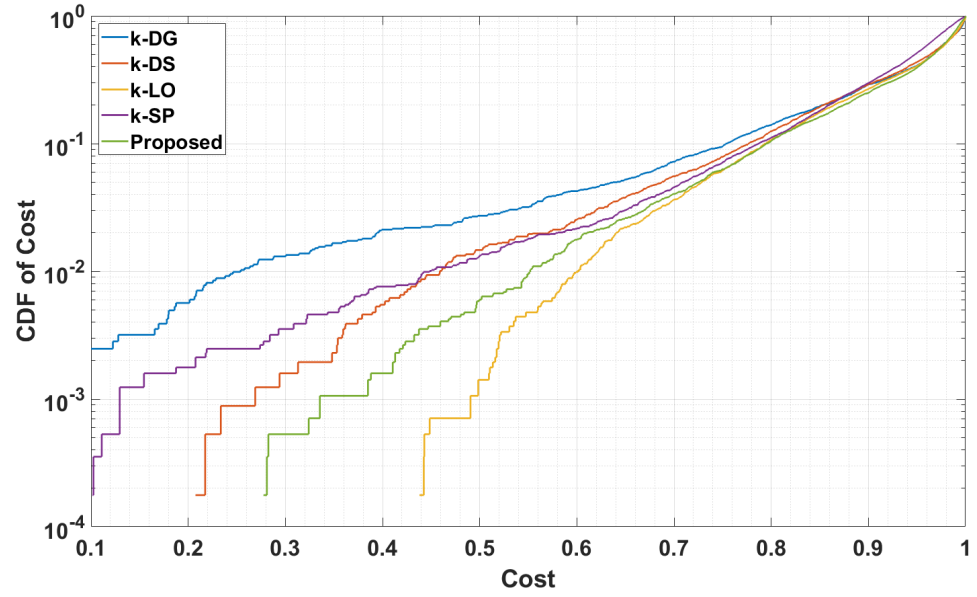

Figure 3. CDF of the attackers' costs of launching DDoS Attack on an LEO satellite network.

It is notable that the k-RAND algorithm provides the highest probability of exceeding a certain cost for the DDoS attack between the cost values from 0.82 to 0.96. Furthermore, it is notable that k-RAND provides optimum results compared to all the other algorithms. The probability that the attacker's cost exceeds the average values (shown in Table 2) is highest for the k-RAND algorithm. Thus, it can provide robustness against the DDoS attacks. Besides, it provides an additional layer of uncertainty to the attacker by the choice

of the algorithm used for routing that would mean an additional probabilistic cost to the attacker.

In Figure 4, we show the histogram plot of the routing algorithm with respect to the detectability/MaxUp. The adversary would not fully occupy the bandwidth of one particular uplink as it would be easily detectable. The MaxUp is normalized to the bandwidth of one uplink, so it will distribute such attacks among multiple uplinks. It is expected that, due to increased uncertainty in the routing algorithm, the detectability of the algorithm will slightly degrade. This can be noticed in the histogram plots. The average median values of the Maxup are shown in Table 3 for all the algorithms. As it can be noted, the k-SP provides the best MaxUp results, however, at the same time, we noted that its average and median costs are not better compared to the k-RAND algorithm. We note that the k-RAND provides the lower median detectability, but it is better than k-DS. At the same time, we note that k-RAND has the highest probability of the cost of attack exceeding the average cost of attack compared to all the algorithms.

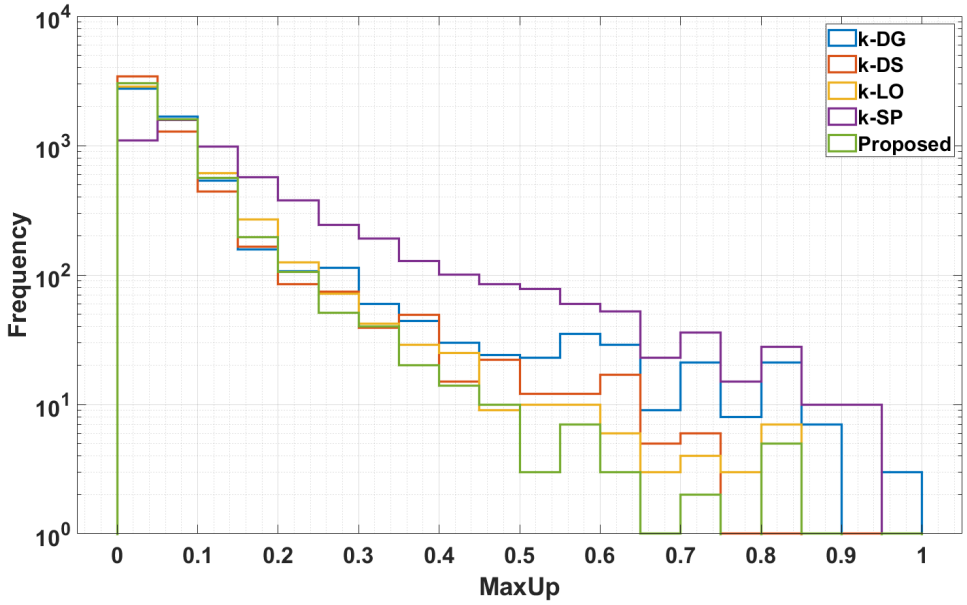

Figure 4. Histogram plot of the attackers' detectability/MaxUp of launching a DDoS Attack on an LEO satellite network.

Table 3. MaxUp Statistics.

Algorithm	Average	Median
k-SP	0.1618	0.1050
k-DG	0.0905	0.0500
k-DS	0.0684	0.0350
k-LO	0.0775	0.0475
k-RAND	0.0690	0.0450

The CDF of the MaxUp is shown in Figure 5. As the CDF plot shows that we have obtained moderate results in the case of the detectability of the algorithm. It is seen that the k-SP is better in terms of detectability, but we have already seen that the proposed algorithm outperforms k-SP in terms of adversary cost. Due to the increased complexity of our algorithm, the detectability is slightly degraded, i.e., if an LSN has an algorithm that produces more predictable routing, a specific link would be more easily congested. On the other hand, for the same reason, it would be easier to detect an attack because a pattern in the routing would stand out more easily.

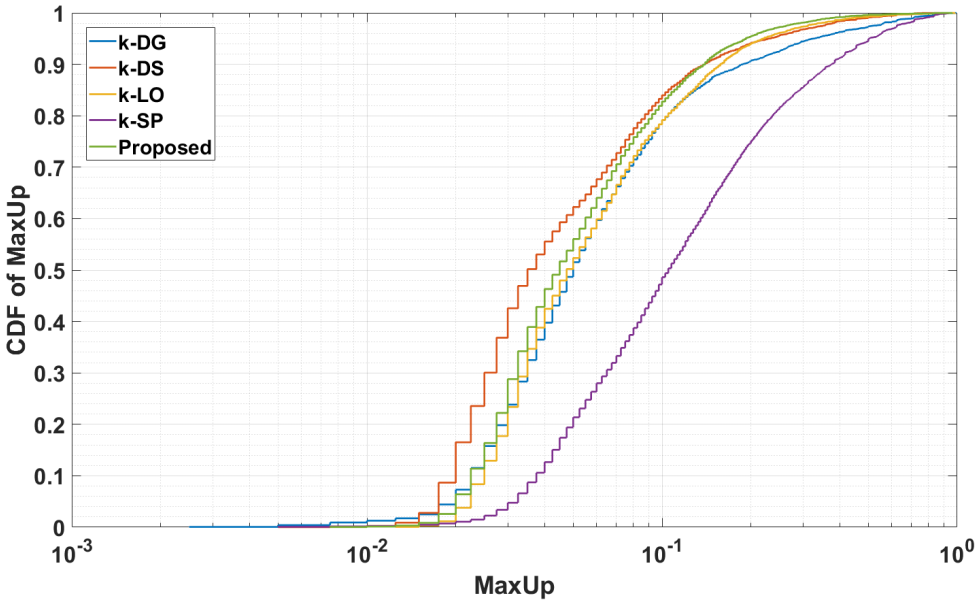

Figure 5. CDF of the attackers' detectability/MaxUp of launching a DDoS Attack on an LEO satellite network.

5. Conclusions

In this article, we have briefly discussed the critical issue of cyberattacks in the context of LEO satellite networks. Recently the LEO network is under various kind of threats and DDoS specifically poses a huge threat. To address DDoS attacks in LSNs, we have proposed a random routing algorithm k-RAND that improves the average and median cost of attack on an LEO satellite network in addition to increasing uncertainty in the routing algorithm. It was shown that the random routing algorithm enhances the attacker's average and median cost while maintaining the functionality of the network but functions at the cost of a slightly degraded detectability performance. The algorithm is based on the selection of one of four classic algorithms—k-LO, k-DS, k-DG, and k-SP—by introducing randomness to the selection with weighted probability distribution. The optimization of the parameters of the k-RAND algorithm that provides the distribution of our algorithm is performed by formulating a Bayesian optimization problem that maximizes the average cost of the DDoS attacks. The k-RAND algorithm will be an effective and robust defensive measure for the DDoS attacks against the modern LEO satellite communication link. The codes used for the simulation studies are available on https://github.com/RubenFr/icarus-framework, (accessed on 18 January 2020).

Author Contributions: For research articles Conceptualization, R.F., Y.S., R.K. and S.A.; Methodology, R.F., Y.S., R.K. and S.A.; Software, R.F. and Y.S.; Validation, R.F., Y.S., R.K. and S.A.; Formal analysis, R.F., Y.S., R.K. and S.A.; Investigation, R.F., Y.S., R.K. and S.A.; Resources, R.F. and Y.S.; Data curation, R.F. and Y.S.; Writing—original draft, R.F., Y.S., R.K. and S.A.; Writing—review & editing, R.F., Y.S., R.K. and S.A.; Visualization, R.F., Y.S., R.K. and S.A.; Supervision, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Kreitman School of Advanced Graduate Studies and Ben-Gurion University of the Negev, Israel for providing fellowships to continue the research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ye, L.; Yang, Y.; Jing, X.; Ma, J.; Deng, L.; Li, H. Single-Satellite Integrated Navigation Algorithm Based on Broadband LEO Constellation Communication Links. *Remote Sens.* **2021**, *13*, 703. [CrossRef]
2. Kumar, R.; Arnon, S. SNR Optimization for LEO Satellite at Sub-THz Frequencies. *IEEE Trans. Antennas Propag.* **2022**, *70*, 4449–4458. [CrossRef]
3. Lee, J.H.; Seo, H.; Park, J.; Bennis, M.; Ko, Y.C. Learning Emergent Random Access Protocol for LEO Satellite Networks. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 257–269. [CrossRef]
4. Esposito, M.; Palma, L.; Belli, A.; Sabbatini, L.; Pierleoni, P. Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review. *Sensors* **2022**, *22*, 2124. [CrossRef]
5. Chen, Y.; Zhang, M.; Li, X.; Che, T.; Jin, R.; Guo, J.; Yang, W.; An, B.; Nie, X. Satellite-Enabled Internet of Remote Things Network Transmits Field Data from the Most Remote Areas of the Tibetan Plateau. *Sensors* **2022**, *22*, 3713. [CrossRef]
6. Li, H.; Shi, D.; Wang, W.; Liao, D.; Gadekallu, T.R.; Yu, K. Secure routing for LEO satellite network survivability. *Comput. Netw.* **2022**, *211*, 109011. [CrossRef]
7. Kumar, R.; Arnon, S. Enhancing Cybersecurity of Satellites at Sub-THz Bands. In *Cyber Security, Cryptology, and Machine Learning*; Dolev, S., Katz, J., Meisels, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 356–365.
8. Giuliari, G.; Ciussani, T.; Perrig, A.; Singla, A. ICARUS: Attacking low earth orbit satellite networks. In Proceedings of the 2021 USENIX Annual Technical Conference (USENIX ATC 21), Online, 14–16 July 2021; pp. 317–331.
9. Lab, K. Collateral Damage: 26% of DDoS Attacks Lead to Data Loss. 2015. Available online: https://www.kaspersky.com/about/press-releases/2015_collateral-damage-26-of-ddos-attacks-lead-to-data-loss (accessed on 23 August 2022).
10. Hildebrand, C. Satellite Companies, ISPs Feeling the Heat from Hackers. 2020. Available online: https://www.netscout.com/blog/satellite-companies-isps-feeling-heat-hackers (accessed on 23 August 2022).
11. Baron, S. Simple Steps To Calculate The Costs Of DDoS Attack—Part 1. 2020. Available online: https://blog.mazebolt.com/calculate-ddos-attack-costs (accessed on 23 August 2022).
12. Al-Hraishawi, H.; Chougrani, H.; Kisseleff, S.; Lagunas, E.; Chatzinotas, S. A Survey on Non-Geostationary Satellite Systems: The Communication Perspective. *IEEE Commun. Surv. Tutor.* **2022**, 1. [CrossRef]
13. Zhang, H.; Ren, D.; Jiang, F. A Beam Search-Based Channel Allocation Method for Interference Mitigation of NGSO Satellites with Multi-Beam Antennas. *Aerospace* **2022**, *9*, 177. [CrossRef]
14. Jia, M.; Zhang, L.; Wu, J.; Guo, Q.; Gu, X. Joint computing and communication resource allocation for edge computing towards Huge LEO networks. *China Commun.* **2022**, *19*, 73–84. [CrossRef]
15. Kumar, R.; Arnon, S. DNN Beamforming for LEO Satellite Communication at Sub-THz Bands. *Electronics* **2022**, *11*, 3937. [CrossRef]
16. Cao, X.; Li, Y.; Xiong, X.; Wang, J. Dynamic Routings in Satellite Networks: An Overview. *Sensors* **2022**, *22*, 4552. [CrossRef] [PubMed]
17. Huang, Y.; Cao, W.; Liu, X.; Jiang, X.; Yang, J.; Yang, F. An Adaptive Multipath Routing for LEO Satellite Network. In Proceedings of the 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 18–20 June 2021; Volume 4, pp. 1536–1541. [CrossRef]
18. Iglesias-Sanuy, P.; López-Ardao, J.C.; Rodríguez-Pérez, M.; Herrería-Alonso, S.; Suárez-González, A.; Rodríguez-Rubio, R.F. An Efficient Location-Based Forwarding Strategy for Named Data Networking and LEO Satellite Communications. *Future Internet* **2022**, *14*, 285. [CrossRef]
19. Madni, M.A.A.; Iranmanesh, S.; Raad, R. DTN and Non-DTN Routing Protocols for Inter-CubeSat Communications: A comprehensive survey. *Electronics* **2020**, *9*, 482. [CrossRef]
20. Chan, C.C.; Al Homssi, B.; Al-Hourani, A. Performance Evaluation of Random Access Methods for IoT-over-Satellite. *Remote Sens.* **2022**, *14*, 4232. [CrossRef]
21. Wang, C.; Wang, H.; Wang, W. A Two-Hops State-Aware Routing Strategy Based on Deep Reinforcement Learning for LEO Satellite Networks. *Electronics* **2019**, *8*, 920. [CrossRef]
22. Xiao, Y.; Liu, J.; Shen, Y.; Jiang, X.; Shiratori, N. Secure Communication in Non-Geostationary Orbit Satellite Systems: A Physical Layer Security Perspective. *IEEE Access* **2019**, *7*, 3371–3382. [CrossRef]
23. Li, Y.; An, K.; Liang, T.; Yan, X. Secrecy Performance of Land Mobile Satellite Systems With Imperfect Channel Estimation and Multiple Eavesdroppers. *IEEE Access* **2019**, *7*, 31751–31761. [CrossRef]
24. Kalantari, A.; Zheng, G.; Gao, Z.; Han, Z.; Ottersten, B. Secrecy Analysis on Network Coding in Bidirectional Multibeam Satellite Communications. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1862–1874. [CrossRef]
25. Zheng, G.; Arapoglou, P.D.; Ottersten, B. Physical Layer Security in Multibeam Satellite Systems. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 852–863. [CrossRef]
26. Bankey, V.; Upadhyay, P.K. Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2488–2501. [CrossRef]
27. Lu, W.; Liang, T.; An, K.; Yang, H. Secure Beamforming and Artificial Noise Algorithms in Cognitive Satellite-Terrestrial Networks With Multiple Eavesdroppers. *IEEE Access* **2018**, *6*, 65760–65771. [CrossRef]
28. Guo, K.; Lin, M.; Zhang, B.; Ouyang, J.; Zhu, W.P. Secrecy Performance of Satellite Wiretap Channels With Multi-User Opportunistic Scheduling. *IEEE Wirel. Commun. Lett.* **2018**, *7*, 1054–1057. [CrossRef]

29. Ai, Y.; Mathur, A.; Cheffena, M.; Bhatnagar, M.R.; Lei, H. Physical Layer Security of Hybrid Satellite-FSO Cooperative Systems. *IEEE Photonics J.* **2019**, *11*, 1–14. [CrossRef]
30. Abdrabou, M.; Gulliver, T.A. Authentication for Satellite Communication Systems Using Physical Characteristics. *IEEE Open J. Veh. Technol.* **2023**, *4*, 48–60. [CrossRef]
31. O'Neill, M.; O'Sullivan, E.; McWilliams, G.; Saarinen, M.J.; Moore, C.; Khalid, A.; Howe, J.; Del Pino, R.; Abdalla, M.; Regazzoni, F.; et al. Secure architectures of future emerging cryptography SAFEcrypto. In Proceedings of the ACM International Conference on Computing Frontiers, Como, Italy, 16–19 May 2016; pp. 315–322.
32. Ostad-Sharif, A.; Abbasinezhad-Mood, D.; Nikooghadam, M. Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications. *Comput. Commun.* **2019**, *147*, 85–97. [CrossRef]
33. Murtaza, A.; Pirzada, S.J.H.; Hasan, M.N.; Xu, T.; Jianwei, L. An Efficient Encryption Algorithm for Perfect Forward Secrecy in Satellite Communication. In *Advances in Cyber Security*; Anbar, M., Abdullah, N., Manickam, S., Eds.; Springer: Singapore, 2020; pp. 289–302.
34. Pirzada, S.J.H.; Murtaza, A.; Xu, T.; Jianwei, L. Architectural Optimization of Parallel Authenticated Encryption Algorithm for Satellite Application. *IEEE Access* **2020**, *8*, 48543–48556. [CrossRef]
35. Nguyen, H.N. *Routing and Quality-of-Service in Broadband LEO Satellite Networks*; Springer: Boston, MA, USA, 2003; Volume 2.
36. Hu, J.; Cai, L.; Zhao, C.; Pan, J. Directed Percolation Routing for Ultra-Reliable and Low-Latency Services in Low Earth Orbit (LEO) Satellite Networks. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 18 November–16 December 2020; pp. 1–6. [CrossRef]
37. Zhao, Z.; Wu, Q.; Li, H.; Lai, Z.; Liu, J. LRAR: A Lightweight Risk-Avoidance Routing Algorithm for LEO Satellite Networks. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 223–228. [CrossRef]
38. Na, Z.Y.; Deng, Z.A.; Chen, N.; Gao, Z.H.; Guo, Q. An active distributed QoS routing for LEO satellite communication network. In Proceedings of the 2015 10th International Conference on Communications and Networking in China (ChinaCom), Shanghai, China, 15–17 August 2015; pp. 538–543. [CrossRef]
39. Manulis, M.; Bridges, C.P.; Harrison, R.; Sekar, V.; Davis, A. Cyber security in New Space. *Int. J. Inf. Secur.* **2020**, *20*, 1–25. [CrossRef]
40. Riahi Manesh, M.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. [CrossRef]
41. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-based communications security: A survey of threats, solutions, and research challenges. *Comput. Netw.* **2022**, *216*, 109246. [CrossRef]
42. Woodard, M.; Sarvestani, S.S.; Hurson, A.R. Chapter Two—A Survey of Research on Data Corruption in Cyber—Physical Critical Infrastructure Systems. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2015; Volume 98, pp. 59–87. [CrossRef]
43. Zhang, Y.; Wang, Y.; Hu, Y.; Lin, Z.; Zhai, Y.; Wang, L.; Zhao, Q.; Wen, K.; Kang, L. Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack. *Sensors* **2022**, *22*, 7286. [CrossRef]
44. Meng, W.; Xue, K.; Xu, J.; Hong, J.; Yu, N. Low-Latency Authentication Against Satellite Compromising for Space Information Network. In Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, 9–12 October 2018; pp. 237–244. [CrossRef]
45. Pavur, J.; Martinovic, I. Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. *J. Cybersecur.* **2022**, *8*, tyac008. [CrossRef]
46. Alabdan, R. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet* **2020**, *12*, 168. [CrossRef]
47. Qi, M.; Chen, J.; Chen, Y. A secure authentication with key agreement scheme using ECC for satellite communication systems. *Int. J. Satell. Commun. Netw.* **2019**, *37*, 234–244. [CrossRef]
48. Alghawazi, M.; Alghazzawi, D.; Alarifi, S. Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 764–777. [CrossRef]
49. Rodríguez, G.E.; Torres, J.G.; Flores, P.; Benavides, D.E. Cross-site scripting (XSS) attacks and mitigation: A survey. *Comput. Netw.* **2020**, *166*, 106960. [CrossRef]
50. Richardson, C.; Reith, M.; Henry, W. Ensuring the Security of Space Systems from Eavesdropping Attacks. In Proceedings of the International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Volume 17, pp. 522–526.
51. Scanlan, J.; Styles, J.; Lyneham, D.; Lutzhoft, M. New Internet Satellite Constellations to Increase Cyber Risk in Ill-Prepared Industries. In Proceedings of the 70th International Astronautical Congress (IAC), Washington, DC, USA, 21–25 October 2019; pp. 1–12.
52. Eppstein, D. Finding the k Shortest Paths. *SIAM J. Comput.* **1998**, *28*, 652–673. [CrossRef]
53. Dong, X.J.; Shi, H.S. A Shortest Path Algorithm Based on Mobile Agent in LEO Satellite Network. In Proceedings of the 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 12–14 October 2008; pp. 1–5. [CrossRef]
54. Eilam-Tzoreff, T. The disjoint shortest paths problem. *Discret. Appl. Math.* **1998**, *85*, 113–138. [CrossRef]
55. Chondrogiannis, T.; Bouros, P.; Gamper, J.; Leser, U.; Blumenthal, D.B. Finding k-shortest paths with limited overlap. *VLDB J.* **2020**, *29*, 1023–1047. [CrossRef]

56. Frazier, P.I. A tutorial on Bayesian optimization. *arXiv* **2018**, arXiv:1807.02811.
57. Nogueira, F. Bayesian Optimization: Open Source Constrained Global Optimization Tool for Python. 2014. Available online: https://github.com/fmfn/BayesianOptimization (accessed on 8 January 2023).